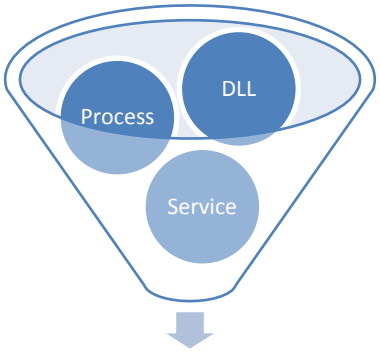
# Volatile and Memory Analysis in a Network Environment

Christopher J. Mellen

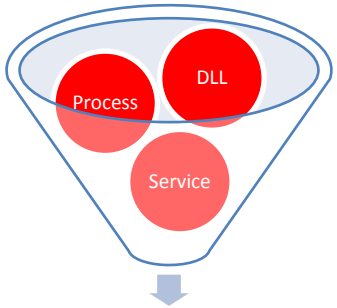
410-703-9237

cmellen@accessdata.com

# What is a Clean Network?



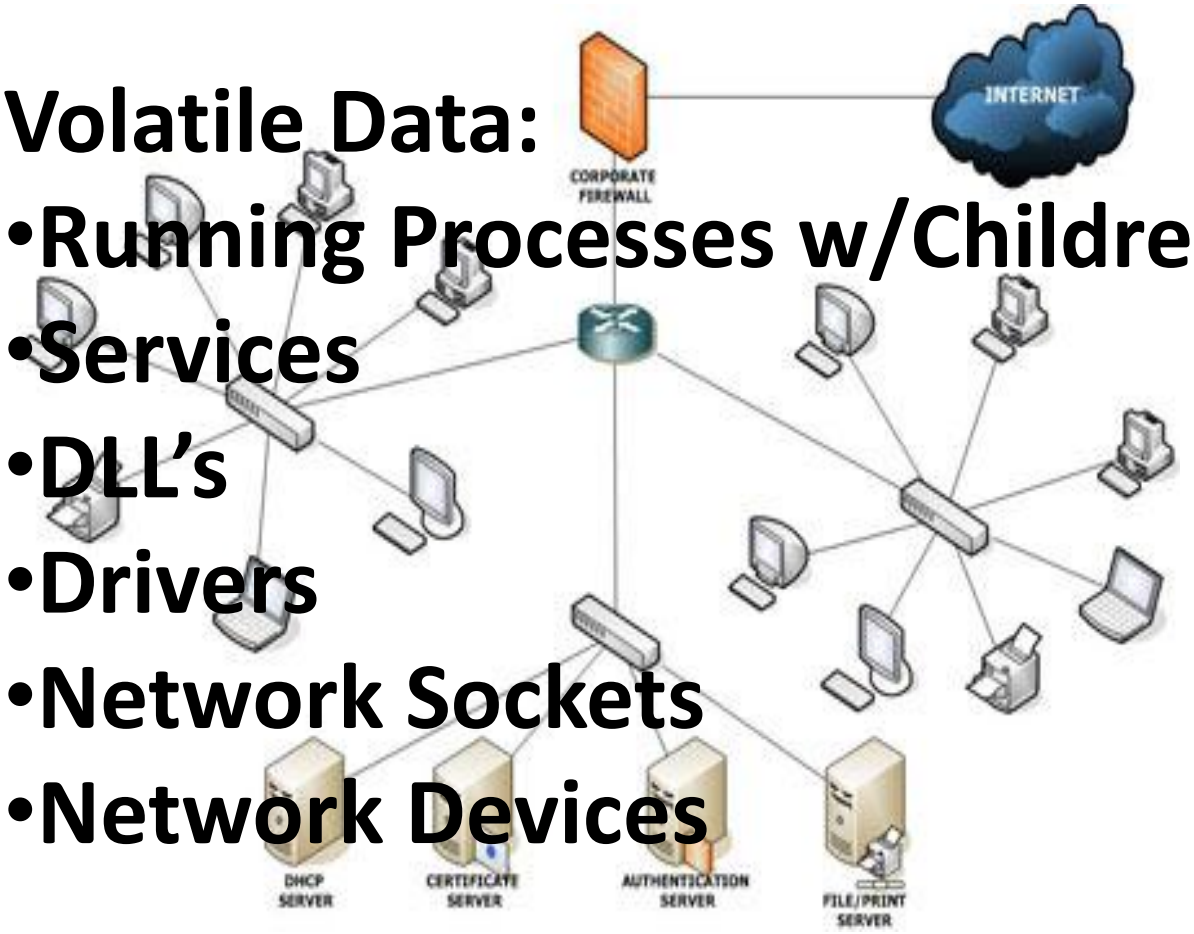

GOOD???

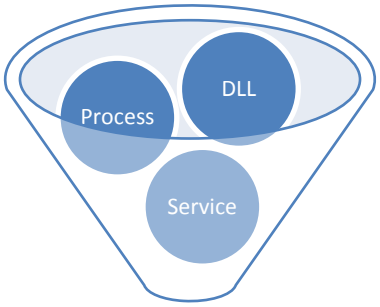



BAD???

**Volatile Data:**

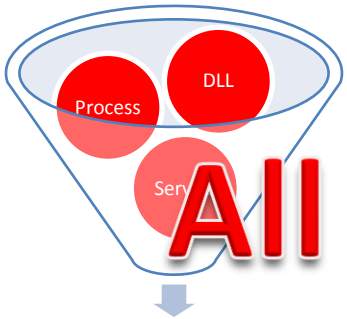
- **Running Processes w/Children**
- **Services**
- **DLL's**
- **Drivers**
- **Network Sockets**
- **Network Devices**






GOOD???

# What is Good?



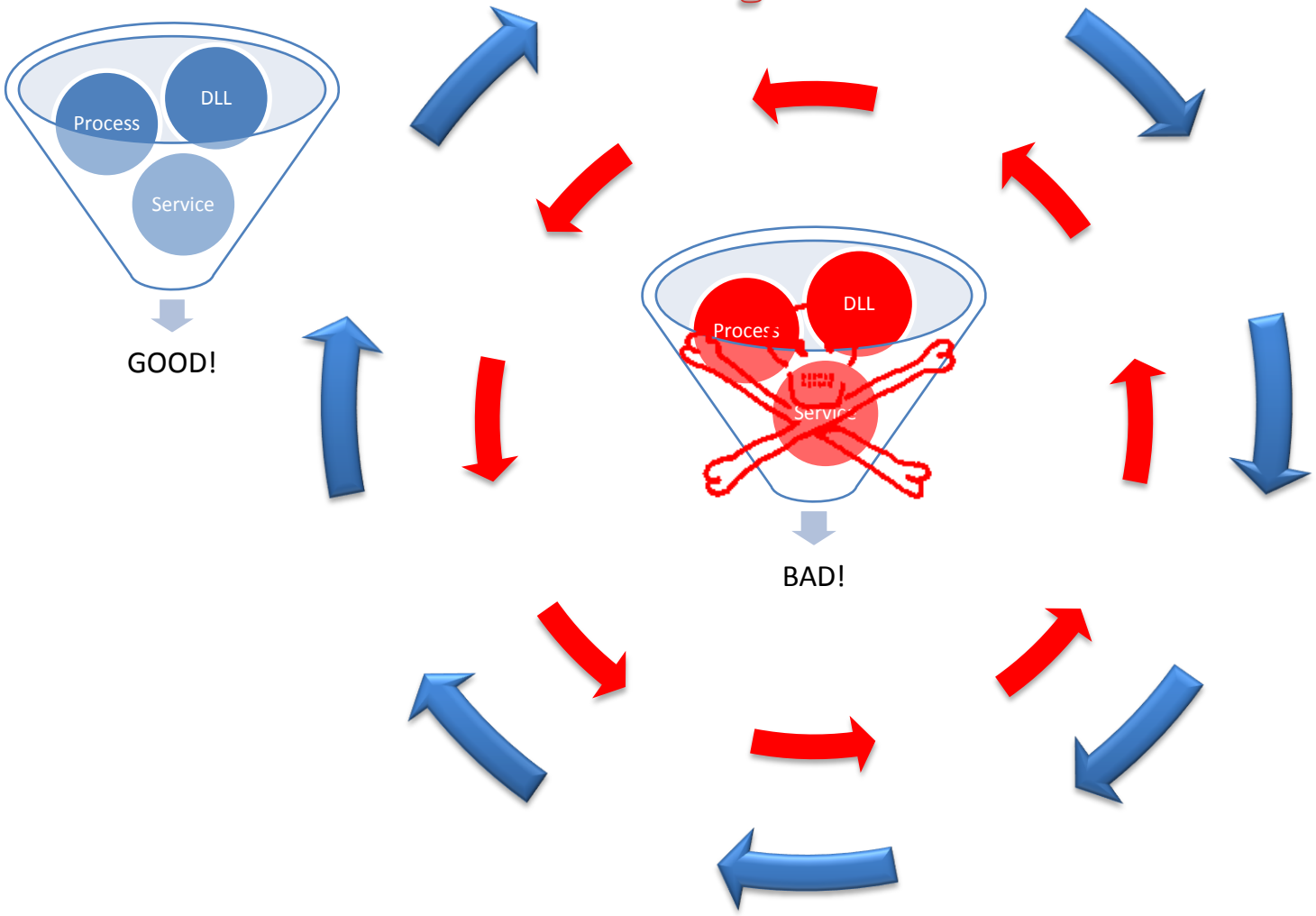

BAD???

# In God We Trust, All Else? We Investigate

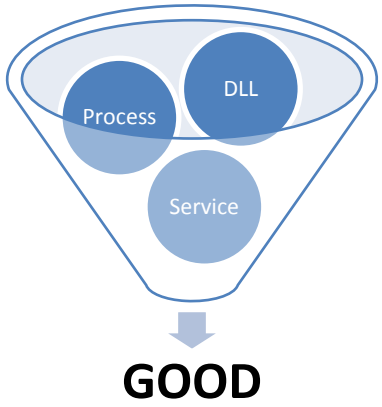
What is Bad?

UNKNOWN = BAD

# How Much "Unknown" is Inside your Network?



# Building a Profile



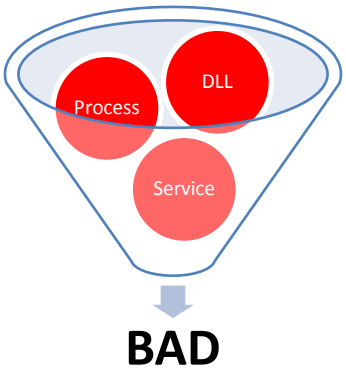

- Obtain Base-Line Builds
- “Best Effort”

- Build Base-Line Profile (Good)

- Known Hash Sets (Good)

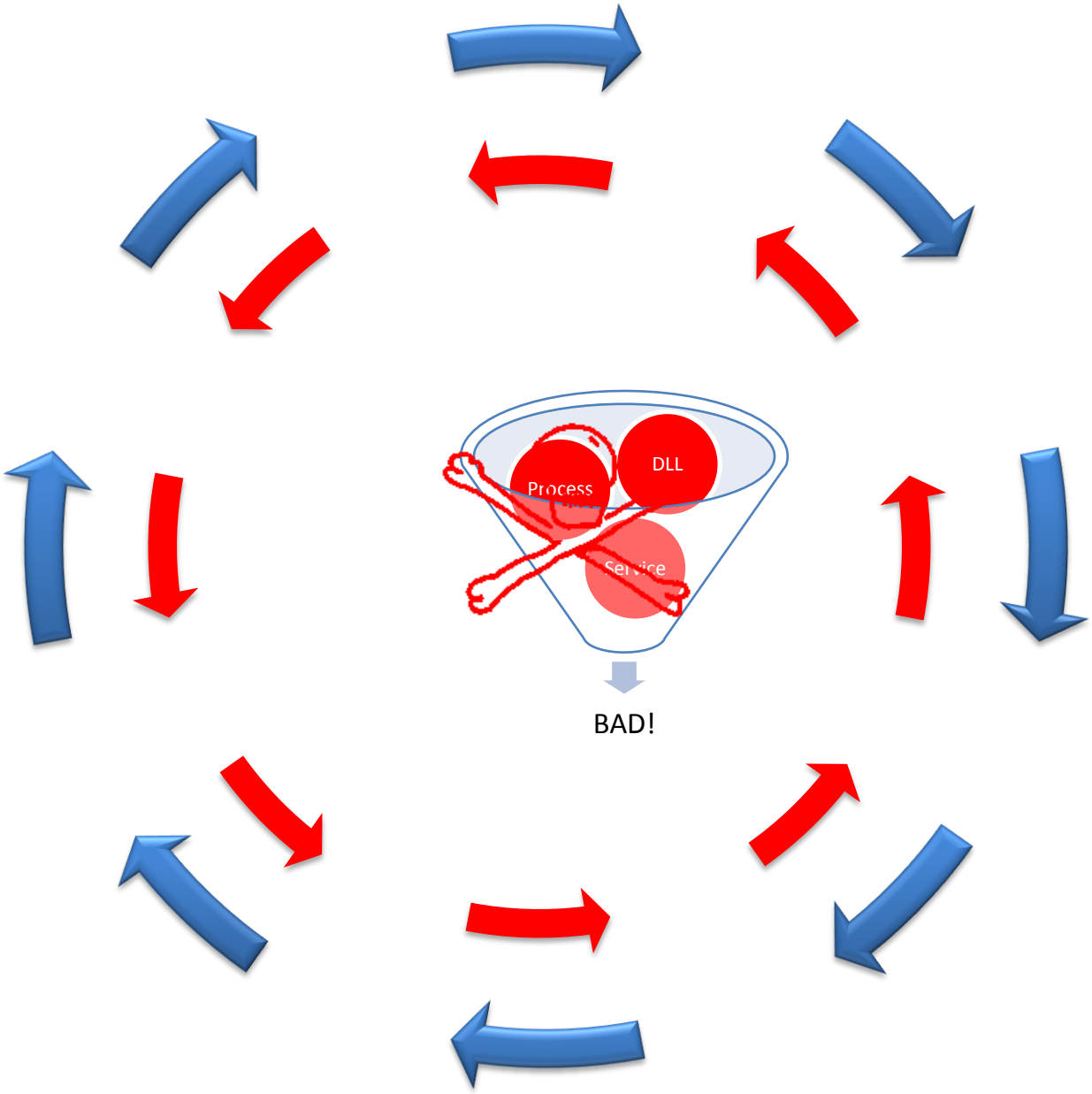
- “Enterprise Profile”

# Building a Profile

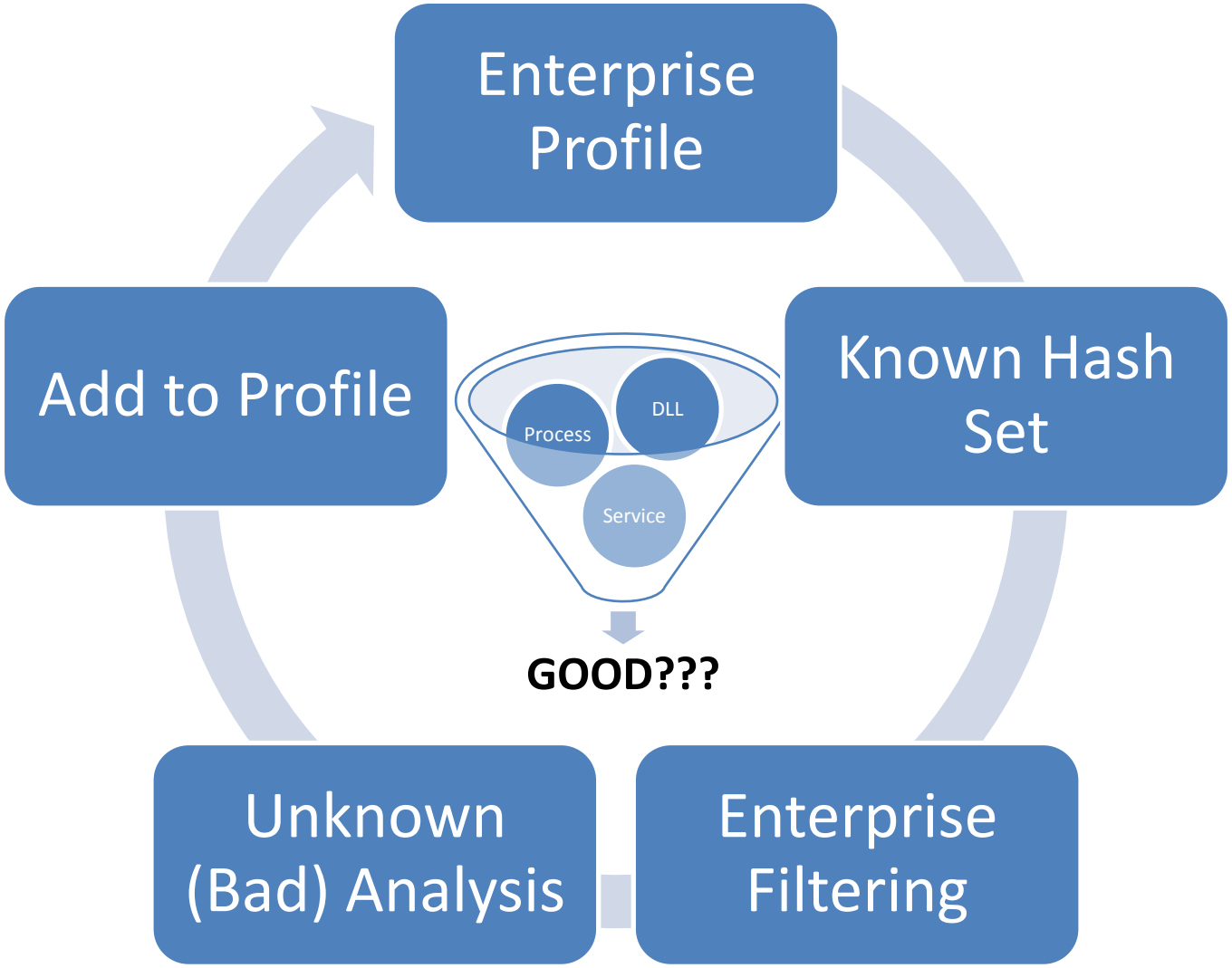


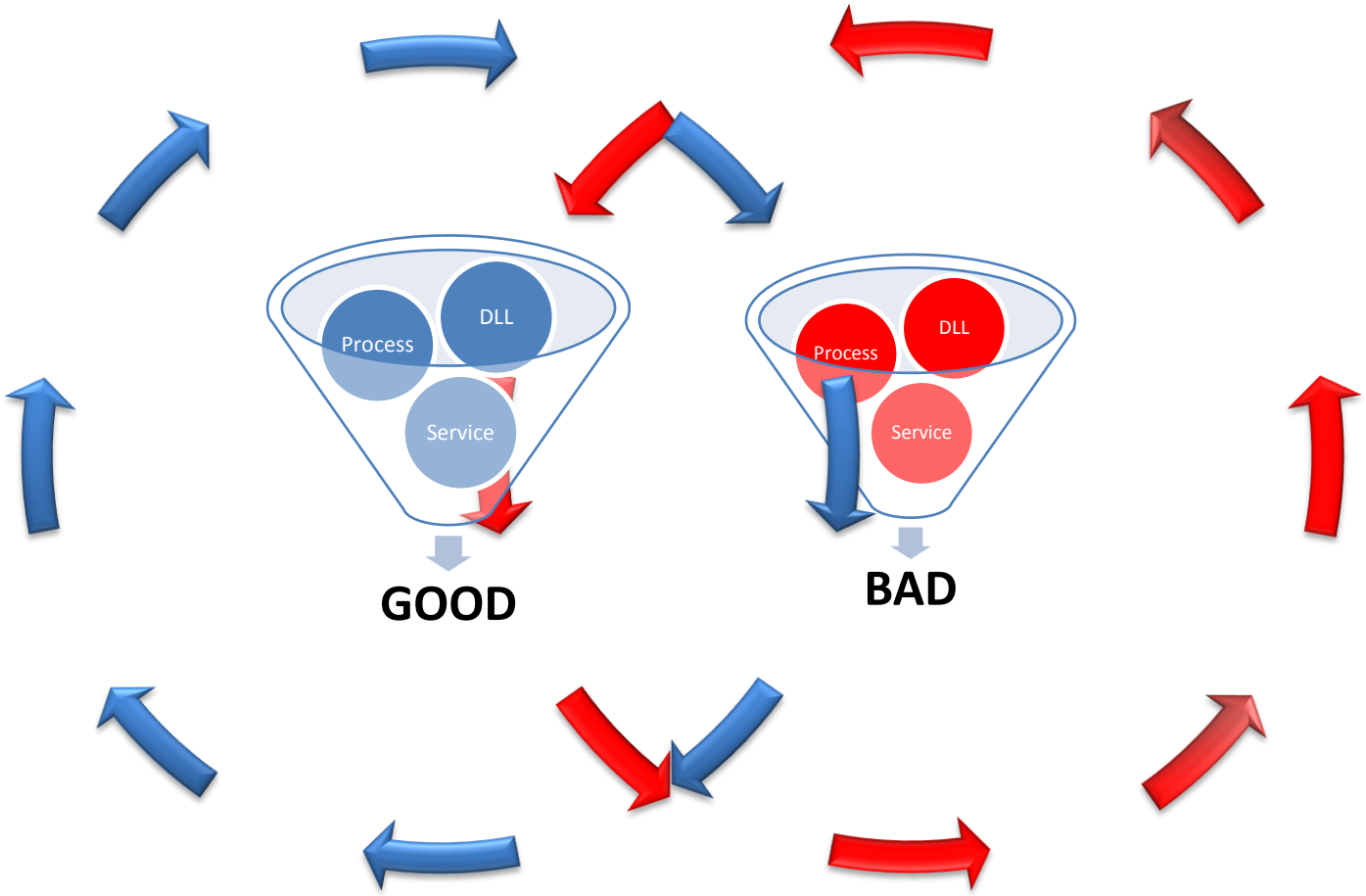

- Known Hash Set (Bad)
- Custom Hash Set (Bad)
- Build Profile

- What's the Problem???


DLL
Process
Service
BAD!

# The Process


Enterprise Profile
Known Hash Set
Enterprise Filtering
Unknown (Bad) Analysis
Add to Profile
Process
DLL
Service
GOOD???


Process
DLL
Service
GOOD
Process
DLL
Service
BAD

# Live Demonstration

# Conclusion

Questions?